IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Daniel BUTTIKER

Application No.: New U. S. Patent Application

Filed: June 29, 2001   Docket No.:   109988

For: METHOD AND TOKEN FOR REGISTERING USERS OF A PUBLIC-KEY
        INFRASTRUCTURE AND REGISTRATION SYSTEM

PRELIMINARY AMENDMENT

Director of the U.S. Patent and Trademark Office
Washington, D. C. 20231

Sir:

Prior to initial examination, please amend the above-identified application as follows:

IN THE CLAIMS:

Please replace claims 3-11 and 14-20 as follows:

3. (Amended) Method according to claim 1, with a serial number of the token being stored in the memory device (5), which, included in the certification request, is sent to the authority (100) which, based on said serial number, retrieves the symmetric or asymmetric key or the password matching the key or password used for signing the biometric data (58) in order to decrypt the signed message.

4. (Amended) Method according to claim 1, for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising the steps of issuing for each token (10) an individual symmetric or asymmetric key-pair, a first key stored in the token (10) for signing the biometric data (58) and a second key (54) stored at the registration authority (101).

5. (Amended) Method according to claim 1, with the public-key (54; 55) of the registration authority (101) and or the certification authority (102) being stored in the token (10), comprising the steps of encrypting at least the part of the certification request containing the biometric data with one of said public-keys (54; 55) before sending it and decrypting the received certification request by the registration authority (101) with the corresponding private-key (53, ...).

6. (Amended) Method according claim 1 with the biometric input device (31) being integrated in the token (10) comprising the steps of pressing a finger onto the token (10) while biometric data (58) is read.

7. (Amended) Method according to claim 1 comprising the steps of storing the biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

8. (Amended) Method according to claim 1 comprising the steps of comparing a password entered with the password stored in the token (10) and/or reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) or in the database (104) of the authority (100) and providing access to the system in case that the compared data match and/or storing mismatched data as proof for legal prosecution of a non-authorised user of the token 10.

9. (Amended) Method according to claim 1 comprising the steps of generating the key pair for the user, the private-key (51) and the public-key (52) within the token (10).

10. (Amended) Method according to claim 1 comprising the steps of performing transactions defined by the authority of the public-key infrastructure while using the registered token (10).

11. (Amended) Method according to claim 1 comprising the steps of keeping the user's data, particularly the biometric data, private except for cases of fraud.

14. (Amended) Token (10) according to claim 12, with a serial number of the token being stored in the memory device (5).

15. (Amended) Token (10) according to claim 12, for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising an individual key of a symmetric or asymmetric key-pair or a shared password for signing the biometric data (58) and a public-key (55) issued by the registration authority (101) or the certification authority (102) for encrypting the certification request sent to the authority (100).

16. (Amended) Token (10) according to claim 12 with the biometric input device (1) being integrated in the token (10).

17. (Amended) Token (10) according to claim 12 designed to store the read biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

18. (Amended) Token (10) according to claim 12 capable to compare a password entered with the password stored in the token (10) and/or capable of reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) providing access to the system in case that the compared data match.

19. (Amended) Token (10) according to claim 12 capable to generating the key pair for the user, the private-key (51) and the public-key (52), within the token (10).
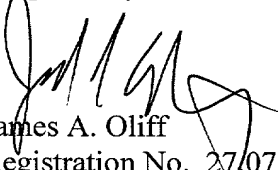
20. (Amended) Registration system (35) providing access to a token (10) according to claim 12 with a terminal (30) designed to exchange data with the network (200) of the public-key infrastructure, with a connected token (10) and with at least one biometric input device (31) capable of reading biometric data, preferably as data related to a fingerprint, the retina, the face and/or the voice of a user which biometric data is transferable via the terminal (30) to the token (10) for processing.

REMARKS

Claims 1 - 20 are pending. By this Preliminary Amendment, claims 3-11 and 14-20 are amended to remove multiple dependencies. Prompt and favorable examination on the merits is respectfully requested.

The attached Appendix includes marked-up copies of each rewritten claim (37 C.F.R. 1.121(c)(1)(ii)).

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/cln

Date: June 29, 2001

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE
AUTHORIZATION
Please grant any extension
necessary for entry;
Charge any fee due to our
Deposit Account No. 15-0461

APPENDIX

Changes to Claims:

The following are marked-up versions of the amended claims:

3. (Amended) Method according to claim 1 or 2, with a serial number of the token being stored in the memory device (5), which, included in the certification request, is sent to the authority (100) which, based on said serial number, retrieves the symmetric or asymmetric key or the password matching the key or password used for signing the biometric data (58) in order to decrypt the signed message.

4. (Amended) Method according to claim 1, 2 or 3 for a public-key infrastructure with an authority (100), consisting of a registration authority (101, a certification authority (102) and a key and certificate management unit (103), comprising the steps of issuing for each token (10) an individual symmetric or asymmetric key-pair, a first key stored in the token (10) for signing the biometric data (58) for a second key (54) stored at the registration authority (101).

5. (Amended) Method according to claim 1, 2, 3 or 4 with the public-key (54: 55) of the registration authority (101) and or the certification authority (102) being stored in the token (10), comprising the steps of encrypting at least the part of the certification request containing the biometric data with one of said public-keys (54; 55) before sending it and decrypting the received certification request by the registration authority (101) with the corresponding private-key (53, ...).

6. (Amended) Method according to one of the claims 1-5 with the biometric input device (31) being integrated in the token (10) comprising the steps of pressing a finger onto the token (10) while biometric data (58) is read.

7. (Amended) Method according to one of the claims 1-6 comprising the steps of storing the biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

8. (Amended) Method according to one of the claims 1 to 7 comprising the steps of comparing a password entered with the password stored in the token (10) and/or reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) or in the database (104) of the authority (100) and providing access to the system in case that the compared data match and/or storing mismatched data as proof for legal prosecution of a non-authorised user of the token 10.

9. (Amended) Method according to one of the claims 1 to 8 comprising the steps of generating the key pair for the user, the private-key (51) and the public-key (52) within the token (10).

10. (Amended) Method according to one of the claims 1 to 9 comprising the steps of performing transactions defined by the authority of the public-key infrastructure while using the registered token (10).

11. (Amended) Method according to one of the claims 1 to 10 comprising the steps of keeping the user's data, particularly the biometric data, private except for cases of fraud.

14. (Amended) Token (10) according to claim 12 or 13, with a serial number of the token being stored in the memory device (5).

15. (Amended) Token (10) according to claim 12 for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising an individual key of a symmetric or asymmetric key-pair or a shared password for signing the biometric data (58) and a public-key (55) issued by the registration authority (101) or the certification authority (102) for encrypting the certification request sent to the authority (100).

16. (Amended) Token (10) according to one of the claims 12-15 with the biometric input device (1) being integrated in the token (10).

17. (Amended) Token (10) according to one of the claims 12-16 designed to store the read biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

18. (Amended) Token (10) according to one of the claims 12-17 capable to compare a password entered with the password stored in the token (10) and/or capable of reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) providing access to the system in case that the compared data match.

19. (Amended) Token (10) according to one of the claims 12-18 capable to generating the key pair for the user, the private-key (51) and the public-key (52), within the token (10).

20. (Amended) Registration system (35) providing access to a token (10) according to one of the claims 12-19 with a terminal (30) designed to exchange data with the network (200) of the public-key infrastructure, with a connected token (10) and with at least one biometric input device (31) capable of reading biometric data, preferably as data related to a fingerprint, the retina, the face and/or the voice of a user which biometric data is transferable via the terminal (30) to the token (10) for processing.